COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 55, No. 2 2006

ed. RIKKYO UNIV/MATH
IKEBUKURO TOKYO
171–8501 JAPAN

Counting Points of the Curve $y^4 = x^3 + a$ over a Finite Field

by

Eiji OZAKI

(Received August 10, 2006)
(Revised October 20, 2006)

Abstract. We give explicit formulas of the number of rational points and of the congruence zeta function for a non-singular complete curve over a finite field defined by an affine equation $y^4 = x^3 + a$.

Introduction

Davenport and Hasse proved a beautiful formula of the congruence zeta function of a non-singular complete curve over a finite field defined by an affine equation $ax^m + by^n = c$, using Jacobi sums. As a consequence the Riemann hypothesis for the congruence zeta function was verified for their case. Their work ascends back to the argument by Gauss in Disquitiones Arithmeticae. In the article, we prove the following formula, starting from the work of Davenport and Hasse.

THEOREM. *Let X be the non-singular complete curve over the finite field $\mathbb{F}_p$ defined by the affine equation $y^4 = x^3 + a$.*

(1) *Suppose $p \equiv 1 \mod 12$. There exist unique pairs of integers (A, B) and (C, D) with*

$$A^2 + 3B^2 = p\,,\ A \equiv 1 \mod 3\,,\ B > 0$$

and

$$C^2 + D^2 = p\,,\ C \equiv 1 \mod 3\,,\ D > 0\,.$$

Put $\pi = A + B\sqrt{-3}$ and $\rho = C + D\sqrt{-1}$, and let χ and η denote the multiplicative character of $\mathbb{F}_p$ defined by $\alpha \mapsto \left(\frac{\alpha}{\pi}\right)_3$ and $\alpha \mapsto \left(\frac{\alpha}{\rho}\right)_4$, respectively. Then we have:

(a1) $\#X(\mathbb{F}_p) = p + 1 - 2A - 4C$ *if* $\chi(a) = 1$ *and* $\eta(a) = 1$;
(a2) $\#X(\mathbb{F}_p) = p + 1 - 2A + 4C$ *if* $\chi(a) = 1$ *and* $\eta(a) = -1$;
(b1) $\#X(\mathbb{F}_p) = p + 1 + 2A + 4D$ *if* $\chi(a) = 1$ *and* $\eta(a) = i$;

*Partially supported by The Research on Security and Reliability in Electronic Society, Chuo University 21st Century COE Program.

2005 *Mathematics Subject Classification* Primary 11G20; Secondary 14G10, 11L05.

(b2) $\#X(\mathbb{F}_p) = p + 1 + 2A - 4D$ *if* $\chi(a) = 1$ *and* $\eta(a) = -i$;
(c1) $\#X(\mathbb{F}_p) = p + 1 + A + 3B + 2C$ *if* $\chi(a) = \omega$ *and* $\eta(a) = 1$;
(c2) $\#X(\mathbb{F}_p) = p + 1 + A + 3B - 2C$ *if* $\chi(a) = \omega$ *and* $\eta(a) = -1$;
(d1) $\#X(\mathbb{F}_p) = p + 1 - A - 3B - 2D$ *if* $\chi(a) = \omega$ *and* $\eta(a) = i$;
(d2) $\#X(\mathbb{F}_p) = p + 1 - A - 3B + 2D$ *if* $\chi(a) = \omega$ *and* $\eta(a) = -i$;
(e1) $\#X(\mathbb{F}_p) = p + 1 + A - 3B + 2C$ *if* $\chi(a) = \omega^2$ *and* $\eta(a) = 1$;
(e2) $\#X(\mathbb{F}_p) = p + 1 + A - 3B - 2C$ *if* $\chi(a) = \omega^2$ *and* $\eta(a) = -1$;
(f1) $\#X(\mathbb{F}_p) = p + 1 - A + 3B - 2D$ *if* $\chi(a) = \omega^2$ *and* $\eta(a) = i$;
(f2) $\#X(\mathbb{F}_p) = p + 1 - A + 3B + 2D$ *if* $\chi(a) = \omega^2$ *and* $\eta(a) = -i$.

(2) *Suppose* $p \equiv 7 \mod 12$. *There exists uniquely a pair of integers* (A, B) *with*

$$A^2 + 3B^2 = p\,,\ A \equiv 1 \mod 3\,,\ B > 0\,.$$

Put $\pi = A + B\sqrt{-3}$, *and let* χ *and* η *denote the multiplicative character of* $\mathbb{F}_p$ *defined by* $\alpha \mapsto \left(\frac{\alpha}{\pi}\right)_3$ *and* $\alpha \mapsto \left(\frac{\alpha}{p}\right)$, *respectively. Then we have*:

(a) $\#X(\mathbb{F}_p) = p + 1 - 2A$ *if* $\chi(a) = 1$ *and* $\eta(a) = 1$;
(b) $\#X(\mathbb{F}_p) = p + 1 + 2A$ *if* $\chi(a) = 1$ *and* $\eta(a) = -1$;
(c) $\#X(\mathbb{F}_p) = p + 1 + A + 3B$ *if* $\chi(a) = \omega$ *and* $\eta(a) = 1$;
(d) $\#X(\mathbb{F}_p) = p + 1 - A - 3B$ *if* $\chi(a) = \omega$ *and* $\eta(a) = -1$;
(e) $\#X(\mathbb{F}_p) = p + 1 + A - 3B$ *if* $\chi(a) = \omega^2$ *and* $\eta(a) = 1$;
(f) $\#X(\mathbb{F}_p) = p + 1 - A + 3B$ *if* $\chi(a) = \omega^2$ *and* $\eta(a) = -1$.

(3) *Suppose* $p \equiv 5$ *or* $11 \mod 12$. *Then we have* $\#X(\mathbb{F}_p) = p + 1$.

Now we explain the contents of the article.

In the section 1, after recalling the definition of power residue symbols and Jacobi sums, we mention a result due to Davenport-Hasse [3] on the congruence zeta function of a non-singular projective curve defined by $ax^m + by^n = c$ over a finite field.

In the section 2, we prove the main theorem. It is not difficult to verify the statement when $p \not\equiv 1 \mod 12$, while the section is mostly devoted to the case of $p \equiv 1 \mod 12$. It is crucial to compare the two formulae

$$\#X(\mathbb{F}_q) = q + 1 + \sum_{\substack{0<i<4\\0<j<3}} \chi^i\left(\frac{c}{a}\right)\eta^j\left(\frac{c}{b}\right)J(\chi^i, \eta^j) \qquad \text{(Davenport-Hasse)}$$

and

$$\#X(\mathbb{F}_p) = \#E(\mathbb{F}_p) + \sum_{\substack{(\alpha,\beta)\in\mathbb{F}_p^2\\ \beta^2=\alpha^3+a}} \left(\frac{\beta}{p}\right),$$

where E denotes the elliptic curve over the finite field $\mathbb{F}_p$ defined by $y^2 = x^3 + a$. This enables us to detremine the Jacobi sums $J(\chi^i, \eta^j)$.

In the secton 3, we determine the congruence zeta function of the non-singular projective curve defined by $y^4 = x^3 + a$ over $\mathbb{F}_p$. The case of $p \equiv 1 \mod 12$ is settled in the

previous section, while the section is mostly devoted to detrmine the Jacobi sums $J(\chi^i, \eta^j)$ over $\mathbb{F}_{p^2}$ when $p \not\equiv 1 \mod 12$.

Acknowledgment. The author expresses his hearty thanks to Professor Noriyuki Suwa for his advices and suggestions. He has learned much from his lecture in the winter semester 2004, getting materials of the section 1. He thanks also Yasuhiro Niitsuma for his careful reading of the manuscript.

Contents

NOTATION. Throughout this article, p denotes a prime number and q a power of p.

$\mathbb{F}_q$**:** the finite field of order q
$\mathbb{F}_q^\times$**:** $\mathbb{F}_q - \{0\}$
$X(\mathbb{F}_q)$**:** the set of $\mathbb{F}_q$-rational points of an algebraic variety X
$\#S$**:** the cardinal of a finite set S

1. Recall: a result of Davenport-Hasse

In this section, we mention a classical result due to Davenport and Hasse, recalling the definition of power residue symbols and Jacobi sums.

1.1. Let $\mathbb{F}_q$ denote the finite field of order q. A multiplicative character of $\mathbb{F}_q$ is nothing but a homomorphism of multiplicative groups $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$. The trivial character ε is defined by $\varepsilon(\alpha) = 1$ for all $\alpha \in \mathbb{F}_q^\times$. By convention, we set

$$\chi(0) = \begin{cases} 1 & \text{if } \chi \text{ is trivial} \\ 0 & \text{if } \chi \text{ is non-trivial} \end{cases}.$$

Then we have

$$\sum_{\alpha \in \mathbb{F}_q} \chi(\alpha) = \begin{cases} q & \text{if } \chi \text{ is trivial} \\ 0 & \text{if } \chi \text{ is non-trivial} \end{cases}.$$

EXAMPLE 1.2. Let n be an integer ≥ 2, and let K be a number field containing all the n-th roots of unity. Take a prime ideal $\mathfrak{p}$ of K, not dividing n. For any integer α of K, prime to $\mathfrak{p}$, there exists uniquely an n-th root of unity $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$ such that

$$\alpha^{\frac{N\mathfrak{p}-1}{n}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_n \mod \mathfrak{p},$$

where $N\mathfrak{p}$ denotes the order of the residue field at $\mathfrak{p}$. We call $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$ the n-th power residue symbol. Put $q = N\mathfrak{p}$. Then $\alpha \mapsto \left(\frac{\alpha}{\mathfrak{p}}\right)_n$ induces a multiplicative character of $\mathbb{F}_q$ of order n.

When $n = 2$, $K = \mathbb{Q}$ and p is a prime number $\neq 2$, the power residue symbol is nothing but the Legendre symbol $\left(\frac{\alpha}{p}\right)$.

1.3. Let χ and η be multiplicative characters of the finite field $\mathbb{F}_q$. The Jacobi sum $J(\chi, \eta)$ is defined by

$$J(\chi, \eta) = \sum_{\alpha \in \mathbb{F}_q} \chi(\alpha)\eta(1-\alpha)\,.$$

It is well known that

(1) $J(\chi, \eta) = J(\eta, \chi)$;
(2) $J(\varepsilon, \varepsilon) = q$;
(3) $J(\chi, \varepsilon) = J(\varepsilon, \chi) = 0$ if χ is non-trivial;
(4) $J(\chi, \chi^{-1}) = -\chi(-1)$ if χ is non-trivial;
(5) $|J(\chi, \eta)| = \sqrt{q}$ if χ, η and $\chi\eta$ are non-trivial.

LEMMA 1.4. *Let n be an integer ≥ 2, and let K be a number field containing all the n-th roots of unity. Take a prime ideal $\mathfrak{p}$ of K and put $q = N\mathfrak{p}$. Let χ denote the multiplicative character of the finite field $\mathbb{F}_q$ induced by $\alpha \mapsto \left(\frac{\alpha}{\mathfrak{p}}\right)_n$. Then we have a congruence relation*

$$J(\chi^i, \chi^j) \equiv 0 \mod \mathfrak{p}$$

if $i > 0$, $j > 0$ and $i + j < n$.

Proof. By the definition, we have

$$J(\chi^i, \chi^j) = \sum_{\alpha \in \mathbb{F}_q} \chi^i(\alpha)\chi^j(1-\alpha) \equiv \sum_{\alpha \in \mathbb{F}_q} \left(\frac{\alpha}{\mathfrak{p}}\right)_n^i \left(\frac{1-\alpha}{\mathfrak{p}}\right)_n^j$$
$$\equiv \sum_{\alpha \in \mathbb{F}_q} \alpha^{\frac{(q-1)i}{n}} (1-\alpha)^{\frac{(q-1)j}{n}} \mod \mathfrak{p}$$

Put $F(u) = u^{\frac{(q-1)i}{n}}(1-u)^{\frac{(q-1)j}{n}} \in \mathbb{Z}[u]$. By the assumption, $F(u)$ has degree $< q-1$ without constant term. Then we have

$$\sum_{\alpha \in \mathbb{F}_q} F(\alpha) = 0\,.$$

1.5. We can now mention a result due to Davenport and Hasse. Let p be a prime number and q a power of p. Let m and n be positive integers dividing $q-1$. Let C denote the non-singular complete curve over $\mathbb{F}_q$ defined by the affine equation $ax^m + by^n = c$

$(a, b, c \in \mathbb{F}_q^\times)$. Take multiplicative characters χ and η of $\mathbb{F}_q$ of order m and n respectively. Then we have

$$Z(C/\mathbb{F}_q, t) = \prod_{\substack{0<i<m \\ 0<j<n \\ \chi^i\eta^j \neq \varepsilon}} \left(1 + \chi^i\left(\frac{c}{a}\right)\eta^j\left(\frac{c}{b}\right)J(\chi^i, \eta^j)\, t\right) \Big/ (1-t)(1-qt)\,.$$

In particular, we obtain

$$\#C(\mathbb{F}_q) = q + 1 + \sum_{\substack{0<i<m \\ 0<j<n \\ \chi^i\eta^j \neq \varepsilon}} \chi^i\left(\frac{c}{a}\right)\eta^j\left(\frac{c}{b}\right)J(\chi^i, \eta^j)\,.$$

EXAMPLE 1.6. Let p be a prime number ≥ 5, and let E denote the elliptic curve defined by $y^2 = x^3 + a$ over the finite field $\mathbb{F}_p$. It is known that:

(1) Suppose $p \equiv 1 \mod 3$. Then there exists uniquely a pair of integers (A, B) such that $A^2 + 3B^2 = p$, $A \equiv 1 \mod 3$ and $B > 0$. Put $\pi = A + B\sqrt{-3}$. Let χ and η denote the multiplicative characters of the finite field $\mathbb{F}_p$ induced by $\alpha \mapsto \left(\frac{\alpha}{\pi}\right)_3$ and by $\alpha \mapsto \left(\frac{\alpha}{p}\right)$, respectively. Moreover put $\omega = (-1 + \sqrt{-3})/2$. Then we have:

(a) $\#E(\mathbb{F}_p) = p + 1 - 2A$ if $\chi(a) = 1$ and $\eta(a) = 1$;
(b) $\#E(\mathbb{F}_p) = p + 1 + 2A$ if $\chi(a) = 1$ and $\eta(a) = -1$;
(c) $\#E(\mathbb{F}_p) = p + 1 + A + 3B$ if $\chi(a) = \omega$ and $\eta(a) = 1$;
(d) $\#E(\mathbb{F}_p) = p + 1 - A - 3B$ if $\chi(a) = \omega$ and $\eta(a) = -1$;
(e) $\#E(\mathbb{F}_p) = p + 1 + A - 3B$ if $\chi(a) = \omega^2$ and $\eta(a) = 1$;
(f) $\#E(\mathbb{F}_p) = p + 1 - A + 3B$ if $\chi(a) = \omega^2$ and $\eta(a) = -1$.

(2) Suppose $p \equiv 2 \mod 3$. Then we have $\#E(\mathbb{F}_p) = p + 1$.

We give a proof of the statement for the reader's convenience. By the definition of E, we have

$$\#E(\mathbb{F}_p) = p + 1 + \sum_{\alpha \in \mathbb{F}_p} \left(\frac{\alpha^3 + a}{p}\right).$$

Suppose $p \equiv 2 \mod 3$. Then we have

$$\sum_{\alpha \in \mathbb{F}_p} \left(\frac{\alpha^3 + a}{p}\right) = \sum_{\alpha \in \mathbb{F}_p} \left(\frac{\alpha}{p}\right) = 0$$

since the map $\alpha \mapsto \alpha^3 + a$ is bijective over $\mathbb{F}_p$.

Suppose now $p \equiv 1 \mod 3$. Then, by the theorem of Davenport-Hasse, we have

$$\#E(\mathbb{F}_p) = p + 1 + \chi(a)\eta(a)J(\chi, \eta) + \chi^2(a)\eta(a)J(\chi^2, \eta)\,,$$

and therefore,

$$\sum_{\alpha\in\mathbb{F}_p}\left(\frac{\alpha^3+a}{p}\right)=\chi(a)\eta(a)J(\chi,\eta)+\chi^2(a)\eta(a)J(\chi^2,\eta)\,.$$

In particular, we have

$$\sum_{\alpha\in\mathbb{F}_p}\left(\frac{\alpha^3+1}{p}\right)=J(\chi,\eta)+J(\chi^2,\eta)\,.$$

It is easily seen from the definition that the Jacobi sum $J(\chi,\eta)$ is an Eisenstein integer, that is, $J(\chi,\eta)\in\mathbb{Z}[\omega]$. We have also

$$J(\chi,\eta)\overline{J(\chi,\eta)}=p$$

as is remarked in 1.3. Moreover we can verify a congruence relation

$$J(\chi,\eta)\equiv 0 \mod \pi\,,$$

applying Lemma 1.4 to $K=\mathbb{Q}(\omega)$, $\mathfrak{p}=(\pi)$, $n=6$, $i=2$, $j=3$. These imply, together with the prime factorization theorem for the ring of Eisenstein integers, that

$$J(\chi,\eta)\in\{\pm\pi,\pm\omega\pi,\pm\omega^2\pi\}\,.$$

Now put

$$R=\left\{\alpha\in\mathbb{F}_p^\times\,;\,\left(\frac{\alpha^3+1}{p}\right)=1\right\},\quad S=\left\{\alpha\in\mathbb{F}_p^\times\,;\,\left(\frac{\alpha^3+1}{p}\right)=-1\right\},$$
$$T=\left\{\alpha\in\mathbb{F}_p^\times\,;\,\left(\frac{\alpha^3+1}{p}\right)=0\right\}$$

and

$$r=\#R,\ s=\#S,\ t=\#T\,.$$

Then we obtain

$$\mathbb{F}_p^\times=R\cup S\cup T$$

and

$$p-1=r+s+t\,.$$

We have also

$$\sum_{\alpha\in\mathbb{F}_p}\left(\frac{\alpha^3+1}{p}\right)=1+\sum_{\alpha\in\mathbb{F}_p^\times}\left(\frac{\alpha^3+1}{p}\right)=1+r-s\,,$$

and therefore

$$\sum_{\alpha\in\mathbb{F}_p}\left(\frac{\alpha^3+1}{p}\right)=2r+t-p+2\,.$$

Furthermore the map $\alpha \mapsto \alpha^3$ is three-to-one on $\mathbb{F}_p^\times$ since $p \equiv 1 \mod 3$. It follows that $r \equiv s \equiv 0 \mod 3$. On the other hand, we have $t = 3$, that is, there exists exactly three elements $\alpha \in \mathbb{F}_p^\times$ such that $\alpha^3 + 1 = 0$ since $\chi(-1) = 1$. Summing up, we have gotten

$$\sum_{\alpha \in \mathbb{F}_p} \left(\frac{\alpha^3 + 1}{p} \right) = 5 - p + 2r \equiv -2 \mod 6,$$

which implies

$$\mathrm{Tr}(J(\chi, \eta)) \equiv -2 \mod 6.$$

Here Tr denotes the trace for the quadratic extension $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$.

Note now that

$$\mathrm{Tr}(\pi) = 2A,\ \mathrm{Tr}(\omega\pi) = -A - 3B,\ \mathrm{Tr}(\omega^2\pi) = -A + 3B,$$

which implies

$$\mathrm{Tr}(\pi) = 2 \mod 6,\ \mathrm{Tr}(\omega\pi) = \mathrm{Tr}(\omega^2\pi) \equiv -1 \mod 6,$$

and

$$\mathrm{Tr}(-\pi) = -2 \mod 6,\ \mathrm{Tr}(-\omega\pi) = \mathrm{Tr}(-\omega^2\pi) \equiv 1 \mod 6.$$

Hence we obtain $J(\chi, \eta) = -\pi$, and therefore,

(a) $\#E(\mathbb{F}_p) = p + 1 + \mathrm{Tr}(-\pi) = p + 1 - 2A$ if $\chi(a) = 1$ and $\eta(a) = 1$;
(b) $\#E(\mathbb{F}_p) = p + 1 + \mathrm{Tr}(\pi) = p + 1 + 2A$ if $\chi(a) = 1$ and $\eta(a) = -1$;
(c) $\#E(\mathbb{F}_p) = p + 1 + \mathrm{Tr}(-\omega\pi) = p + 1 + A + 3B$ if $\chi(a) = \omega$ and $\eta(a) = 1$;
(d) $\#E(\mathbb{F}_p) = p + 1 + \mathrm{Tr}(\omega\pi) = p + 1 - A - 3B$ if $\chi(a) = \omega$ and $\eta(a) = -1$;
(e) $\#E(\mathbb{F}_p) = p + 1 + \mathrm{Tr}(-\omega^2\pi) = p + 1 + A - 3B$ if $\chi(a) = \omega^2$ and $\eta(a) = 1$;
(f) $\#E(\mathbb{F}_p) = p + 1 + \mathrm{Tr}(\omega^2\pi) = p + 1 - A + 3B$ if $\chi(a) = \omega^2$ and $\eta(a) = -1$.

REMARK 1.7. Let $P(E; t)$ denote the characteristic polynomial of the Frobenius on E over $\mathbb{F}_p$. The assertion of Example 1.6 is restated as follows:

(1) Suppose $p \equiv 1 \mod 6$. There exists uniquely a pair of integers (A, B) with

$$A^2 + 3B^2 = p,\ A \equiv 1 \mod 3,\ B > 0.$$

Put $\pi = A + B\sqrt{-3}$, and let χ and η denote the multiplicative character of $\mathbb{F}_p$ defined by $\alpha \mapsto \left(\frac{\alpha}{\pi}\right)_3$ and $\alpha \mapsto \left(\frac{\alpha}{p}\right)$, respectively. Then we have:

(a) $P(E; t) = 1 - 2At + pt^2$ if $\chi(a) = 1$ and $\eta(a) = 1$;
(b) $P(E; t) = 1 + 2At + pt^2$ if $\chi(a) = 1$ and $\eta(a) = -1$;
(c) $P(E; t) = 1 + (A + 3B)t + pt^2$ if $\chi(a) = \omega$ and $\eta(a) = 1$;
(d) $P(E; t) = 1 - (A + 3B)t + pt^2$ if $\chi(a) = \omega$ and $\eta(a) = -1$;
(e) $P(E; t) = 1 + (A - 3B)t + pt^2$ if $\chi(a) = \omega^2$ and $\eta(a) = 1$;
(f) $P(E; t) = 1 - (A - 3B)t + pt^2$ if $\chi(a) = \omega^2$ and $\eta(a) = -1$.

(2) Suppose $p \equiv 5 \mod 6$. Then we have $P(E; t) = 1 + pt^2$.

COROLLARY 1.8. *Let p be a prime number ≥ 5, and let E denote the elliptic curve over $\mathbb{F}_p$ defined by $y^2 = x^3 + 1$. Then we have*:

(1) $\#E(\mathbb{F}_p) \equiv 0 \mod 12$ *if* $p \not\equiv 5 \mod 12$;
(2) $\#E(\mathbb{F}_p) \equiv 6 \mod 12$ *if* $p \equiv 5 \mod 12$.

Proof. The result follows immediately from the assertion of Example 1.6 when $p \equiv 5 \mod 6$.

Assume now $p \equiv 1 \mod 6$, and take $A, B \in \mathbb{Z}$ so that $A^2 + 3B^2 = p$ and $A \equiv 1 \mod 3$. Then we have $\#E(\mathbb{F}_p) = p + 1 - 2A$ as is shown in Example 1.6. If $p \equiv 1 \mod 12$, then $A \equiv 1 \mod 6$ and $B \equiv 0 \mod 2$, which implies $p + 1 - 2A \equiv 0 \mod 12$. On the other hand, if $p \equiv 7 \mod 12$, then $A \equiv 4 \mod 6$ and $B \equiv 1 \mod 2$, which implies $p + 1 - 2A \equiv 0 \mod 12$.

REMARK 1.9. Let p be a prime number ≥ 5, and let E denote the elliptic curve over $\mathbb{F}_p$ defined by $y^2 = x^3 + 1$. Then we have $\#E(\mathbb{F}_{p^2}) \equiv 0 \mod 12$.

Proof. The reslut follows immediately from 1.7 when $p \not\equiv 5 \mod 12$. If $p \equiv 5 \mod 12$, then we have $\#E(\mathbb{F}_{p^2}) = p^2 + 1 + 2p = (p+1)^2 \equiv 0 \mod 12$.

REMARK 1.10. Let p be a prime number ≥ 5, and let E denote the elliptic curve over $\mathbb{F}_p$ defined by $y^2 = x^3 + a$. As is well known, if $p \equiv 1 \mod 6$, the elliptic curve E is ordinary and the endomorphism ring $\mathrm{End}_{\mathbb{F}_p} E$ is isomorphic to the ring of Eisenstein integers $\mathbb{Z}[\omega]$. On the other hand, if $p \equiv 5 \mod 6$, the elliptic curve E is supersingular.

2. Proof of the main theorem

2.1. We start to prove the main theorem by the following observation. Let E denote the elliptic curve over the finite field $\mathbb{F}_p$ defined by $y^2 = x^3 + a$. Then a double covering $f : X \to E$ is defined by $f(x, y) = (x, y^2)$. Moreover we have

$$\#X(\mathbb{F}_p) = \#E(\mathbb{F}_p) + \sum_{\substack{(\alpha,\beta)\in\mathbb{F}_p^2 \\ \beta^2=\alpha^3+a}} \left(\frac{\beta}{p}\right).$$

2.2. Proof of (3). The map $\alpha \mapsto \alpha^3$ is bijective on $\mathbb{F}_p^\times$ since $p \equiv 2 \mod 3$. Hence we have

$$\sum_{\substack{(\alpha,\beta)\in\mathbb{F}_p^2 \\ \beta^2=\alpha^3+a}} \left(\frac{\beta}{p}\right) = \sum_{\substack{(\alpha,\beta)\in\mathbb{F}_p^2 \\ \beta^2=\alpha}} \left(\frac{\beta}{p}\right) = \sum_{\beta\in\mathbb{F}_p} \left(\frac{\beta}{p}\right) = 0.$$

Hence we obtain that $\#X(\mathbb{F}_p) = \#E(\mathbb{F}_p)$, and the result follows from Example 1.6 (2).

2.3. Proof of (2). We have $\left(\frac{-\beta}{p}\right) = -\left(\frac{\beta}{p}\right)$ for each $\beta \in \mathbb{F}_p^\times$ since $p \equiv 3 \mod 4$. Hence we obtain

$$\sum_{\substack{(\alpha,\beta)\in\mathbb{F}_p^2 \\ \beta^2=\alpha^3+a}} \left(\frac{\beta}{p}\right) = 0\,.$$

This implies that $\#X(\mathbb{F}_p) = \#E(\mathbb{F}_p)$, and the result follows from Example 1.6 (1).

We present Lemma 2.4 and Corollary 2.5, which are necesary to verify (1) of the main theorem and to prove the theorem stated in the next section.

LEMMA 2.4. *Let* $\mathfrak{p}$ *be a prime ideal of* $\mathbb{Q}(e^{\frac{\pi i}{6}})$. *Assume that* $\mathfrak{p}$ *is prime to* 6, *and put* $q = N\mathfrak{p}$. *Let* χ *and* η *denote the multiplicative character of* $\mathbb{F}_q$ *defined by* $\alpha \mapsto \left(\frac{\alpha}{\mathfrak{p}}\right)_3$ *and* $\alpha \mapsto \left(\frac{\alpha}{\mathfrak{p}}\right)_4$, *respectively. Then we have*:

$$\mathrm{Tr}(\chi(a)\eta(a)J(\chi,\eta)) = \sum_{\substack{(\alpha,\beta)\in\mathbb{F}_q^2 \\ \beta^2=\alpha^3+a}} \left(\frac{\beta}{\mathfrak{p}}\right)_2,$$

where Tr *denotes the trace for the extension* $\mathbb{Q}(e^{\frac{\pi i}{6}})/\mathbb{Q}$.

Proof. Let X denote the non-singular complete curve over $\mathbb{F}_q$ defined by $y^4 = x^3 + a$ and E the elliptic curve over $\mathbb{F}_q$ defined by $y^2 = x^3 + a$. Applying the theorem of Davenport-Hasse to the curves X and E, we obtain

$$\begin{aligned}\#X(\mathbb{F}_q) = q + 1 &+ \chi(a)\eta^2(a)J(\chi,\eta^2) + \chi^2(a)\eta^2(a)J(\chi^2,\eta^2) \\ &+ \chi(a)\eta(a)J(\chi,\eta) + \chi^2(a)\eta(a)J(\chi^2,\eta) + \chi(a)\eta^3(a)J(\chi,\eta^3) \\ &+ \chi^2(a)\eta^3(a)J(\chi^2,\eta^3)\end{aligned}$$

and

$$\#E(\mathbb{F}_q) = q + 1 + \chi(a)\eta^2(a)J(\chi,\eta^2) + \chi^2(a)\eta^2(a)J(\chi^2,\eta^2)\,.$$

It follows that

$$\#X(\mathbb{F}_q) = \#E(\mathbb{F}_q) + \mathrm{Tr}(\chi(a)\eta(a)J(\chi,\eta))$$

since the orbit of $\chi(a)\eta(a)J(\chi,\eta)$ under the action by $\mathrm{Gal}(\mathbb{Q}(e^{\frac{\pi i}{6}})/\mathbb{Q})$ is given by

$$\{\chi(a)\eta(a)J(\chi,\eta),\ \chi^2(a)\eta(a)J(\chi^2,\eta),\ \chi(a)\eta^3(a)J(\chi,\eta^3),\ \chi^2(a)\eta^3(a)J(\chi^2,\eta^3)\}\,.$$

On the other hand, we have

$$\#X(\mathbb{F}_q) = \#E(\mathbb{F}_q) + \sum_{\substack{(\alpha,\beta)\in\mathbb{F}_q^2 \\ \beta^2=\alpha^3+a}} \left(\frac{\beta}{\mathfrak{p}}\right)_2.$$

Hence the result.

COROLLARY 2.5. *Under the notations of 2.4, we have*

$$\mathrm{Tr}(J(\chi,\eta)) \equiv -4 \mod 12\,.$$

Proof. Put

$$R = \left\{(\alpha,\beta) \in \mathbb{F}_q^2\ ;\ \beta^2 = \alpha^3+1,\ \left(\frac{\beta}{\mathfrak{p}}\right)_2 = 1\right\},$$
$$S = \left\{(\alpha,\beta) \in \mathbb{F}_q^2\ ;\ \beta^2 = \alpha^3+1,\ \left(\frac{\beta}{\mathfrak{p}}\right)_2 = -1\right\},$$
$$T = \left\{(\alpha,\beta) \in \mathbb{F}_q^2\ ;\ \beta^2 = \alpha^3+1,\ \left(\frac{\beta}{\mathfrak{p}}\right)_2 = 0\right\}$$

and

$$r = \#R,\ s = \#S,\ t = \#T\,.$$

Let E_1 be the elliptic curve over $\mathbb{F}_q$ defined by $y^2 = x^3+1$. Then we have

$$E_1(\mathbb{F}_q) - \{\infty\} = R \cup S \cup T$$

and

$$\#E_1(\mathbb{F}_q) - 1 = r + s + t\,,$$

where This implies that

$$\sum_{\substack{(\alpha,\beta)\in\mathbb{F}_q^2\\ \beta^2=\alpha^3+1}} \left(\frac{\beta}{\mathfrak{p}}\right)_2 = r - s = 2r + t - \#E_1(\mathbb{F}_q) + 1\,.$$

Hence we obtain the result from (i) $r \equiv 2 \mod 6$; (ii) $t = 3$; (iii) $\#E_1(\mathbb{F}_q) \equiv 0 \mod 12$.

To verify (i), note at first that we have a partition

$$R = \left\{(\alpha,\beta) \in (\mathbb{F}_q^\times)^2\ ;\ \beta^2 = \alpha^3+1,\ \left(\frac{\beta}{\mathfrak{p}}\right)_2 = 1\right\} \cup \{(0,\pm 1)\}$$

since $q \equiv 1 \mod 4$. Moreover the group $\boldsymbol{\mu}_3 \times \boldsymbol{\mu}_2$ acts faithfully on $R - \{(0,\pm 1)\}$ by $(\zeta,\theta)(\alpha,\beta) = (\zeta\alpha, \theta\beta)$ since $\left(\frac{-\beta}{\mathfrak{p}}\right)_2 = \left(\frac{\beta}{\mathfrak{p}}\right)_2$ for each $\beta \in \mathbb{F}_q$.

It is easy to verify (ii), In fact, there exist exactly three elements $\alpha \in \mathbb{F}_q^\times$ such that $\alpha^3+1 = 0$ since $q \equiv 1 \mod 6$. The assertion (iii) follows from Corollary 1.8 and Remark 1.9.

2.6. Proof of (1). We have a prime factorization

$$(p) = (\pi,\rho)(\pi,\bar\rho)(\bar\pi,\rho)(\bar\pi,\bar\rho)$$

in $\mathbb{Q}(e^{\frac{\pi i}{6}}) = \mathbb{Q}(\sqrt{-1},\sqrt{-3})$, and it is readily seen that:

(a) $\left(\frac{\alpha}{(\pi,\rho)}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3$ for any $\alpha \in \mathbb{Z}[\omega]$;

(b) $\left(\frac{\alpha}{(\pi,\rho)}\right)_4 = \left(\frac{\alpha}{\rho}\right)_4$ for any $\alpha \in \mathbb{Z}[\sqrt{-1}]$.

Hence, applying the theorem of Davenport-Hasse to the curves X and E over $\mathbb{F}_p$, we obtain

$$\#X(\mathbb{F}_p) = \#E(\mathbb{F}_p) + \mathrm{Tr}(\chi(a)\eta(a)J(\chi,\eta))$$

as in the proof of Lemma 2.4.

In the next paragraph, we shall verify

$$(\#) \qquad J(\chi,\eta) = J(\chi^2,\eta) = -\rho,\ J(\chi,\eta^3) = J(\chi^2,\eta^3) = -\bar{\rho}\,,$$

from which the statement of the theorem is deduced as follows. We have

$$\mathrm{Tr}(\rho) = 4C,\ \mathrm{Tr}(i\rho) = -4D,\ \mathrm{Tr}(\omega\rho) = \mathrm{Tr}(\omega^2\rho) = -2C,\ \mathrm{Tr}(i\omega\rho) = \mathrm{Tr}(i\omega^2\rho) = 2D$$

since $\rho = C + D\sqrt{-1}$. Hence, using the result mentioned in Example 1.6, we obtain:

(a1) $\#X(\mathbb{F}_p) = \#E(\mathbb{F}_p) + \mathrm{Tr}(-\rho) = p + 1 - 2A - 4C$ if $\chi(a) = 1$ and $\eta(a) = 1$;

(a2) $\#X(\mathbb{F}_p) = \#E(\mathbb{F}_p) + \mathrm{Tr}(\rho) = p + 1 - 2A + 4C$ if $\chi(a) = 1$ and $\eta(a) = -1$;

(b1) $\#X(\mathbb{F}_p) = \#E(\mathbb{F}_p) + \mathrm{Tr}(-i\rho) = p + 1 + 2A + 4D$ if $\chi(a) = 1$ and $\eta(a) = i$;

(b2) $\#X(\mathbb{F}_p) = \#E(\mathbb{F}_p) + \mathrm{Tr}(i\rho) = p + 1 + 2A - 4D$ if $\chi(a) = 1$ and $\eta(a) = -i$;

(c1) $\#X(\mathbb{F}_p) = \#E(\mathbb{F}_p) + \mathrm{Tr}(-\omega\rho) = p + 1 + A + 3B + 2C$ if $\chi(a) = \omega$ and $\eta(a) = 1$;

(c2) $\#X(\mathbb{F}_p) = \#E(\mathbb{F}_p) + \mathrm{Tr}(\omega\rho) = p + 1 + A + 3B - 2C$ if $\chi(a) = \omega$ and $\eta(a) = -1$;

(d1) $\#X(\mathbb{F}_p) = \#E(\mathbb{F}_p) + \mathrm{Tr}(-i\omega\rho) = p + 1 - A - 3B - 2D$ if $\chi(a) = \omega$ and $\eta(a) = i$;

(d2) $\#X(\mathbb{F}_p) = \#E(\mathbb{F}_p) + \mathrm{Tr}(i\omega\rho) = p + 1 - A - 3B + 2D$ if $\chi(a) = \omega$ and $\eta(a) = -i$;

(e1) $\#X(\mathbb{F}_p) = \#E(\mathbb{F}_p) + \mathrm{Tr}(-\omega^2\rho) = p + 1 + A - 3B + 2C$ if $\chi(a) = \omega^2$ and $\eta(a) = 1$;

(e2) $\#X(\mathbb{F}_p) = \#E(\mathbb{F}_p) + \mathrm{Tr}(\omega^2\rho) = p + 1 + A - 3B - 2C$ if $\chi(a) = \omega^2$ and $\eta(a) = -1$;

(f1) $\#X(\mathbb{F}_p) = \#E(\mathbb{F}_p) + \mathrm{Tr}(-i\omega^2\rho) = p + 1 - A + 3B - 2D$ if $\chi(a) = \omega^2$ and $\eta(a) = i$;

(f2) $\#X(\mathbb{F}_p) = \#E(\mathbb{F}_p) + \mathrm{Tr}(i\omega^2\rho) = p + 1 - A + 3B + 2D$ if $\chi(a) = \omega^2$ and $\eta(a) = -i$.

2.7. Proof of (#). By the definition, the Jacobi sum $J(\chi,\eta)$ is an integer in $\mathbb{Q}(e^{\frac{\pi i}{6}})$. We have a congruence relation

$$J(\chi,\eta) \equiv 0 \mod (\pi,\rho)\,,$$

applying Lemma 1.4 to $K = \mathbb{Q}(e^{\frac{\pi i}{6}})$, $\mathfrak{p} = (\pi,\rho)$, $n = 12$, $i = 4$, $j = 3$. Moreover it holds that

$$\left(\frac{\alpha}{(\bar{\pi},\rho)}\right)_3 = \left(\frac{\alpha}{\bar{\pi}}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3^{-1}$$

for any $\alpha \in \mathbb{Z}$. Then we have a congruence relation

$$J(\chi,\eta) \equiv 0 \mod (\bar{\pi},\rho)\,,$$

applying Lemma 1.4 to $K = \mathbb{Q}(e^{\frac{\pi i}{6}})$, $\mathfrak{p} = (\bar{\pi}, \rho)$, $n = 12$, $i = 8$, $j = 3$. Combining the two congruence relations, we obtain

$$J(\chi, \eta) \equiv 0 \mod \rho .$$

Hence we can conclude that

$$J(\chi, \eta) \in \{\pm\rho, \pm i\rho, \pm\omega\rho, \pm\omega^2\rho, \pm i\omega\rho, \pm i\omega^2\rho\}$$

since $|J(\chi, \eta)| = \sqrt{p}$ and $|\rho| = \sqrt{p}$.

By Corollary 2.5, we have

$$\operatorname{Tr} J(\chi, \eta) \equiv -4 \mod 12 .$$

On the other hand, we have

$$\operatorname{Tr}(\rho) = 4C,\ \operatorname{Tr}(i\rho) = -4D,\ \operatorname{Tr}(\omega\rho) = \operatorname{Tr}(\omega^2\rho) = -2C,\ \operatorname{Tr}(i\omega\rho) = \operatorname{Tr}(i\omega^2\rho) = 2D .$$

Then we obtain

$$\operatorname{Tr}(\rho) \equiv 4 \mod 12,\ \operatorname{Tr}(-\rho) \equiv -4 \mod 12,\ \operatorname{Tr}(i\rho) \equiv \operatorname{Tr}(-i\rho) \equiv 0 \mod 12$$

since $C \equiv 1 \mod 3$, $D \equiv 0 \mod 3$. We have also, if $C \equiv 1 \mod 6$ and $D \equiv 0 \mod 6$,

$$\operatorname{Tr}(\omega\rho) = \operatorname{Tr}(\omega^2\rho) \equiv -2 \mod 12,\ \operatorname{Tr}(-\omega\rho) = \operatorname{Tr}(-\omega^2\rho) \equiv 2 \mod 12$$

$$\operatorname{Tr}(i\omega\rho) = \operatorname{Tr}(i\omega^2\rho) \equiv \operatorname{Tr}(-i\omega\rho) = \operatorname{Tr}(-i\omega^2\rho) \equiv 0 \mod 12$$

and, if $C \equiv 4 \mod 6$ and $D \equiv 3 \mod 6$,

$$\operatorname{Tr}(\omega\rho) = \operatorname{Tr}(\omega^2\rho) \equiv 4 \mod 12,\ \operatorname{Tr}(-\omega\rho) = \operatorname{Tr}(-\omega^2\rho) \equiv -4 \mod 12 ,$$

$$\operatorname{Tr}(i\omega\rho) = \operatorname{Tr}(i\omega^2\rho) \equiv \operatorname{Tr}(-i\omega\rho) = \operatorname{Tr}(-i\omega^2\rho) \equiv 6 \mod 12 .$$

Then we can conclude

$$J(\chi, \eta) = -\rho$$

or

$$J(\chi, \eta) \in \{-\omega\rho, -\omega^2\rho\},\ C \equiv 4 \mod 6,\ D \equiv 3 \mod 6 .$$

Take now $a \in \mathbb{F}_p$ so that $\chi(a) = 1$ and $\left(\frac{a}{p}\right) = -1$, and put

$$R = \left\{(\alpha, \beta) \in \mathbb{F}_p^2\ ;\ \beta^2 = \alpha^3 + a,\ \left(\frac{\beta}{p}\right) = 1\right\},$$

$$S = \left\{(\alpha, \beta) \in \mathbb{F}_p^2\ ;\ \beta^2 = \alpha^3 + a,\ \left(\frac{\beta}{p}\right) = -1\right\},$$

$$T = \left\{(\alpha, \beta) \in \mathbb{F}_p^2\ ;\ \beta^2 = \alpha^3 + a,\ \left(\frac{\beta}{p}\right) = 0\right\}$$

and

$$r = \#R,\ s = \#S,\ t = \#T .$$

Then we obtain

$$\sum_{\substack{(\alpha,\beta)\in\mathbb{F}_p^2\\ \beta^2=\alpha^3+a}} \left(\frac{\beta}{p}\right) = r - s = 2r + t - \#E(\mathbb{F}_p) + 1$$

as in the proof of Corollary 2.5. Here E is the elliptic curve over $\mathbb{F}_p$ defined by $y^2 = x^3+a$.

We have

$$R = \left\{(\alpha, \beta) \in (\mathbb{F}_p^{\times})^2 \ ; \ \beta^2 = \alpha^3 + a, \ \left(\frac{\beta}{p}\right) = 1\right\}$$

since $\left(\dfrac{a}{p}\right) = -1$. Hence we obtain $r \equiv 0 \mod 6$ since the group $\boldsymbol{\mu}_3 \times \boldsymbol{\mu}_2$ acts faithfully on R by $(\zeta, \theta)(\alpha, \beta) = (\zeta\alpha, \theta\beta)$. We have also $t = 3$ since $\chi(a) = 1$.

Moreover we have $\#E(\mathbb{F}_p) = p + 1 + 2A \equiv 4 \mod 12$ by the statement mentioned in Example 1.6. Summing up, we obtain

$$\mathrm{Tr}(\pm i J(\chi, \eta)) = \sum_{\substack{(\alpha,\beta)\in\mathbb{F}_p^2\\ \beta^2=\alpha^3+a}} \left(\frac{\beta}{p}\right) = 2r + t - \#E(\mathbb{F}_p) + 1 \equiv 0 \mod 12$$

by Lemma 2.4. Hence we can exclude the possibility $J(\chi, \eta) \in \{-\omega\rho, -\omega^2\rho\}$, $C \equiv 4 \mod 6$, $D \equiv 3 \mod 6$, because, otherwise we would have $\mathrm{Tr}(\pm i J(\chi, \eta)) \equiv 6 \mod 12$.

EXAMPLE 2.8. Let $p = 13$. Then we have $(A, B) = (1, 2)$ and $(C, D) = (-2, 3)$, and therefore, $\pi = 1 + 2\sqrt{-3}$ and $\rho = -2 + 3\sqrt{-1}$. Note now that we have

$$7^2 = 10, \ 7^3 = 5, \ 7^4 = 9, \ 7^5 = 11, \ 7^6 = 12, \ 7^7 = 6, \ 7^8 = 3, \ 7^9 = 8, \ 7^{10} = 4, \ 7^{11} = 2$$

in $\mathbb{F}_{13}$. Hence we see that

$$\left(\frac{1}{\pi}\right)_3 = 1, \ \left(\frac{7}{\pi}\right)_3 = \omega, \ \left(\frac{10}{\pi}\right)_3 = \omega^2, \ \left(\frac{5}{\pi}\right)_3 = 1, \ \left(\frac{9}{\pi}\right)_3 = \omega, \ \left(\frac{11}{\pi}\right)_3 = \omega^2,$$
$$\left(\frac{12}{\pi}\right)_3 = 1, \ \left(\frac{6}{\pi}\right)_3 = \omega, \ \left(\frac{3}{\pi}\right)_3 = \omega^2, \ \left(\frac{8}{\pi}\right)_3 = 1, \ \left(\frac{4}{\pi}\right)_3 = \omega, \ \left(\frac{2}{\pi}\right)_3 = \omega^2$$

since $7^4 \equiv 9 \equiv \omega \mod \pi$. On the other hand, we see that

$$\left(\frac{1}{\rho}\right)_4 = 1, \ \left(\frac{7}{\rho}\right)_4 = i, \ \left(\frac{10}{\rho}\right)_4 = -1, \ \left(\frac{5}{\rho}\right)_4 = -i,$$
$$\left(\frac{9}{\rho}\right)_4 = 1, \ \left(\frac{11}{\rho}\right)_4 = i, \ \left(\frac{12}{\rho}\right)_4 = -1, \ \left(\frac{6}{\rho}\right)_4 = -i,$$
$$\left(\frac{3}{\rho}\right)_4 = 1, \ \left(\frac{8}{\rho}\right)_4 = i, \ \left(\frac{4}{\rho}\right)_4 = -1, \ \left(\frac{2}{\rho}\right)_4 = -i$$

since $7^3 = 5 \equiv i \mod \rho$. Hence we obtain:

(a1) $\#X(\mathbb{F}_p) = p + 1 - 2A - 4C = 20$ if $a = 1$;

(a2) $\#X(\mathbb{F}_p) = p + 1 - 2A + 4C = 4$ if $a = 12$;

(b1) $\#X(\mathbb{F}_p) = p + 1 + 2A + 4D = 28$ if $a = 8$;

(b2) $\#X(\mathbb{F}_p) = p + 1 + 2A - 4D = 4$ if $a = 5$;
(c1) $\#X(\mathbb{F}_p) = p + 1 + A + 3B + 2C = 17$ if $a = 9$;
(c2) $\#X(\mathbb{F}_p) = p + 1 + A + 3B - 2C = 25$ if $a = 4$;
(d1) $\#X(\mathbb{F}_p) = p + 1 - A - 3B - 2D = 1$ if $a = 7$;
(d2) $\#X(\mathbb{F}_p) = p + 1 - A - 3B + 2D = 13$ if $a = 6$;
(e1) $\#X(\mathbb{F}_p) = p + 1 + A - 3B + 2C = 5$ if $a = 3$;
(e2) $\#X(\mathbb{F}_p) = p + 1 + A - 3B - 2C = 13$ if $a = 10$;
(f1) $\#X(\mathbb{F}_p) = p + 1 - A + 3B - 2D = 13$ if $a = 11$;
(f2) $\#X(\mathbb{F}_p) = p + 1 - A + 3B + 2D = 25$ if $a = 2$.

REMARK 2.9. In [2], Ch.3.5, the Jacobi sums $J(\chi^i, \eta^j)$ are determined in a different way. We have given here another proof, clarifying a geometric significance of the Jacobi sums.

3. Congruence zeta functions

THEOREM 3.1. *Let X be the non-singular complete curve over the finite field $\mathbb{F}_p$ defined by the affine equation $y^4 = x^3 + a$. Put*

$$P(t) = (1-t)(1-pt)Z(X/\mathbb{F}_p, t)\,.$$

(1) *Suppose $p \equiv 1 \mod 12$. There exist uniquely pairs of integers (A, B) and (C, D) with*

$$A^2 + 3B^2 = p,\ A \equiv 1 \mod 3,\ B > 0$$

and

$$C^2 + D^2 = p,\ C \equiv 1 \mod 3,\ D > 0\,.$$

Put $\pi = A + B\sqrt{-3}$ and $\rho = C + D\sqrt{-1}$, and let χ and η denote the multiplicative character of $\mathbb{F}_p$ defined by $\alpha \mapsto \left(\frac{\alpha}{\pi}\right)_3$ and $\alpha \mapsto \left(\frac{\alpha}{\rho}\right)_4$, respectively. Then we have:

(a1) $P(t) = (1 - 2At + pt^2)(1 - 2Ct + pt^2)^2$ *if* $\chi(a) = 1$ *and* $\eta(a) = 1$;
(a2) $P(t) = (1 - 2At + pt^2)(1 + 2Ct + pt^2)^2$ *if* $\chi(a) = 1$ *and* $\eta(a) = -1$;
(b1) $P(t) = (1 + 2At + pt^2)(1 + 2Dt + pt^2)^2$ *if* $\chi(a) = 1$ *and* $\eta(a) = i$;
(b2) $P(t) = (1 + 2At + pt^2)(1 - 2Dt + pt^2)^2$ *if* $\chi(a) = 1$ *and* $\eta(a) = -i$;
(c1) $P(t) = \{1 + (A + 3B)t + pt^2\}\{1 + 2Ct + (-p + 4C^2)t^2 + 2pCt^3 + p^2t^4\}$ *if* $\chi(a) = \omega$ *and* $\eta(a) = 1$;
(c2) $P(t) = \{1 + (A + 3B)t + pt^2\}\{1 - 2Ct + (-p + 4C^2)t^2 - 2pCt^3 + p^2t^4\}$ *if* $\chi(a) = \omega$ *and* $\eta(a) = -1$;
(d1) $P(t) = \{1 - (A + 3B)t + pt^2\}\{1 - 2Dt + (-p + 4D^2)t^2 - 2pDt^3 + p^2t^4\}$ *if* $\chi(a) = \omega$ *and* $\eta(a) = i$;
(d2) $P(t) = \{1 - (A + 3B)t + pt^2\}\{1 + 2Dt + (-p + 4D^2)t^2 + 2pDt^3 + p^2t^4\}$ *if* $\chi(a) = \omega$ *and* $\eta(a) = -i$;

(e1) $P(t) = \{1 + (A - 3B)t + pt^2\}\{1 + 2Ct + (-p + 4C^2)t^2 + 2pCt^3 + p^2t^4\}$ *if* $\chi(a) = \omega^2$ *and* $\eta(a) = 1$;

(e2) $P(t) = \{1 + (A - 3B)t + pt^2\}\{1 - 2Ct + (-p + 4C^2)t^2 - 2pCt^3 + p^2t^4\}$ *if* $\chi(a) = \omega^2$ *and* $\eta(a) = -1$;

(f1) $P(t) = \{1 - (A - 3B)t + pt^2\}\{1 - 2Dt + (-p + 4C^2)t^2 - 2pDt^3 + p^2t^4\}$ *if* $\chi(a) = \omega^2$ *and* $\eta(a) = i$;

(f2) $P(t) = \{1 - (A - 3B)t + pt^2\}\{1 + 2Dt + (-p + 4C^2)t^2 + 2pDt^3 + p^2t^4\}$ *if* $\chi(a) = \omega^2$ *and* $\eta(a) = -i$.

(2) *Suppose* $p \equiv 5 \mod 12$. *There exists uniquely a pair of integers* (C, D) *with*

$$C^2 + D^2 = p,\ C \equiv 1 \mod 6,\ D \equiv 4 \mod 6.$$

Then we have:

(a) $P(t) = (1 + pt^2)(1 + 4CDt^2 + p^2t^4)$ *if* $\left(\frac{a}{p}\right) = 1$;

(b) $P(t) = (1 + pt^2)(1 - 4CDt^2 + p^2t^4)$ *if* $\left(\frac{a}{p}\right) = -1$.

(3) *Suppose* $p \equiv 7 \mod 12$. *There exists uniquely a pair of integers* (A, B) *with*

$$A^2 + 3B^2 = p,\ A \equiv 1 \mod 3,\ B > 0.$$

Put $\pi = A + B\sqrt{-3}$, *and let* χ *and* η *denote the multiplicative character of* $\mathbb{F}_p$ *defined by* $\alpha \mapsto \left(\frac{\alpha}{\pi}\right)_3$ *and* $\alpha \mapsto \left(\frac{\alpha}{p}\right)$, *respectively. Then we have*:

(a) $P(t) = (1 - 2At + pt^2)(1 - pt^2)^2$ *if* $\chi(a) = 1$ *and* $\eta(a) = 1$;

(b) $P(t) = (1 + 2At + pt^2)(1 - pt^2)^2$ *if* $\chi(a) = 1$ *and* $\eta(a) = -1$;

(c) $P(t) = \{1 + (A + 3B)t + pt^2\}(1 + pt^2 + p^2t^4)$ *if* $\chi(a) = \omega$ *and* $\eta(a) = 1$;

(d) $P(t) = \{1 - (A + 3B)t + pt^2\}(1 + pt^2 + p^2t^4)$ *if* $\chi(a) = \omega$ *and* $\eta(a) = -1$;

(e) $P(t) = \{1 + (A - 3B)t + pt^2\}(1 + pt^2 + p^2t^4)$ *if* $\chi(a) = \omega^2$ *and* $\eta(a) = 1$;

(f) $P(t) = \{1 - (A - 3B)t + pt^2\}(1 + pt^2 + p^2t^4)$ *if* $\chi(a) = \omega^2$ *and* $\eta(a) = -1$.

(4) *Suppose* $p \equiv 11 \mod 12$. *Then we have* $P(t) = (1 + pt^2)^3$.

REMARK 3.2. Let k be a field of characteristic $\neq 2, 3$. Let X denote the non-singular complete curve defined by $y^4 = x^3 + a$ over k, and E the elliptic curve defined by $y^2 = x^3 + a$ over k. Let $J(X)$ denote the Jacobian variety of X. Then the double covering $X \to E$ defined by $(x, y) \mapsto (x, y^2)$ induces a homomorphism of abelian varieties $E \to J(X)$. Put $S = \mathrm{Coker}[E \to J(X)]$. Then S is an abelian surface over k, and $J(X)$ is isogenous to the product $E \times S$.

Assume now $k = \mathbb{F}_q$. Let $P(E/k; t)$ and $P(S/k; t)$ denote the characteristic polynomial of the Frobenius on E and S over k, respectively. Then we have

$$(1 - t)(1 - qt)Z(X/k; t) = P(E/k; t)P(S/k; t).$$

3.3. Proof of (1). By the theorem of Davenport-Hasse, we have

$$P(t) = \prod_{\substack{0<i<3 \\ 0<j<4}} (1 + \chi^i(a)\eta^j(a)J(\chi^i, \eta^j)\, t).$$

Furthermore we have

$$J(\chi,\eta)=J(\chi^2,\eta)=-(C+D\sqrt{-1}),\ J(\chi,\eta^2)=-(A+B\sqrt{-3})$$

and therefore

$$J(\chi^2,\eta^3)=J(\chi,\eta^3)=-(C-D\sqrt{-1}),\ J(\chi^2,\eta^2)=-(A-B\sqrt{-3})$$

as is proved in 2.6 and 1.6. Hence we obtain the result, expanding the right hand side in each case.

3.4. Proof of (3). First note that the prime ideals (π) and $(\bar{\pi})$ of $\mathbb{Q}(\sqrt{-3})$ inert in the extension $\mathbb{Q}(e^{\frac{\pi i}{6}})/\mathbb{Q}(\sqrt{-3})$, and we have a prime factorization $(p)=(\pi)(\bar{\pi})$ in $\mathbb{Q}(e^{\frac{\pi i}{6}})$. Let $\tilde{\chi}$ and η denote the multiplicative character of $\mathbb{F}_{p^2}$ defined by $\alpha\mapsto\left(\frac{\alpha}{\pi}\right)_3$ and $\alpha\mapsto\left(\frac{\alpha}{\pi}\right)_4$, repsectively.

By the definition, the Jacobi sum $J(\tilde{\chi},\eta)$ is an integer in $\mathbb{Q}(e^{\frac{\pi i}{6}})$. We have a congruence relation

$$J(\tilde{\chi},\eta)\equiv 0 \mod \pi\,,$$

applying Lemma 1.4 to $K=\mathbb{Q}(e^{\frac{\pi i}{6}})$, $\mathfrak{p}=(\pi)$, $n=12$, $i=4$, $j=3$.

Define now $\sigma\in\mathrm{Gal}(\mathbb{Q}(e^{\frac{\pi i}{6}})/\mathbb{Q})$ by $\sigma(e^{\frac{\pi i}{6}})=e^{\frac{5\pi i}{6}}$. Then the subfield $\mathbb{Q}(\sqrt{-1})$ of $\mathbb{Q}(e^{\frac{\pi i}{6}})$ is invariant under the action by σ, and $\sigma(\pi)=\bar{\pi}$. It follows that

$$\left(\frac{\alpha}{\bar{\pi}}\right)_3=\left(\frac{\alpha}{\pi}\right)_3^{-1},\ \left(\frac{\alpha}{\bar{\pi}}\right)_4=\left(\frac{\alpha}{\pi}\right)_4$$

for any $\alpha\in\mathbb{Z}[\sqrt{-1}]$. Hence we have a congruence relation

$$J(\tilde{\chi},\eta)\equiv 0 \mod \bar{\pi}\,,$$

applying Lemma 1.4 to $K=\mathbb{Q}(e^{\frac{\pi i}{6}})$, $\mathfrak{p}=(\bar{\pi})$, $n=12$, $i=8$, $j=3$.

Combining the two congruence relations, we obtain

$$J(\tilde{\chi},\eta)\equiv 0 \mod p\,.$$

Hence we can conclude that

$$J(\chi,\eta)\in\{\pm p,\pm ip,\pm\omega p,\pm\omega^2 p,\pm i\omega p,\pm i\omega^2 p\}$$

since $|J(\chi,\eta)|=p$.

By Corollary 2.5, we have

$$\mathrm{Tr}\,J(\tilde{\chi},\eta)\equiv -4 \mod 12\,.$$

On the other hand, we have

$$\mathrm{Tr}(p)=4p,\ \mathrm{Tr}(-p)=-4p,\ \mathrm{Tr}(ip)=\mathrm{Tr}(-ip)=0\,,$$

$$\mathrm{Tr}(\omega p)=\mathrm{Tr}(\omega^2 p)=-p,\ \mathrm{Tr}(-\omega p)=\mathrm{Tr}(-\omega^2 p)=p\,,$$

$$\mathrm{Tr}(i\omega p)=\mathrm{Tr}(i\omega^2 p)=\mathrm{Tr}(-i\omega p)=\mathrm{Tr}(-i\omega^2 p)=0\,,$$

and therefore,

$$\mathrm{Tr}(p) \equiv 4 \mod 12,\ \mathrm{Tr}(-p) \equiv -4 \mod 12\,,$$

$$\mathrm{Tr}(\omega p) = \mathrm{Tr}(\omega^2 p) \equiv 5 \mod 12,\ \mathrm{Tr}(-\omega p) = \mathrm{Tr}(-\omega^2 p) \equiv -5 \mod 12$$

since $p \equiv 7 \mod 12$. These imply

$$J(\tilde{\chi}, \eta) = J(\tilde{\chi}^2, \eta) = J(\tilde{\chi}, \eta^3) = J(\tilde{\chi}^2, \eta^3) = -p\,.$$

Let now $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ denote the eigenvalues of the Frobenius on the abelian surface $S = \mathrm{Coker}[E \to J(X)]$ over $\mathbb{F}_p$. For any $a \in \mathbb{F}_p$, we have $\eta(a) = 1$ and $\tilde{\chi}(a) = \chi^2(a)$ since $p + 1 \equiv 8 \mod 12$. Hence, if $\chi(a) = 1$, we have

$$\{\alpha_1^2, \alpha_2^2, \alpha_3^2, \alpha_4^2\} = \{-J(\tilde{\chi}, \eta), -J(\tilde{\chi}^2, \eta), -J(\tilde{\chi}, \eta^3), -J(\tilde{\chi}^2, \eta^3)\} = \{p, p, p, p\}\,,$$

and therefore

$$\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} = \{\sqrt{p}, -\sqrt{p}, \sqrt{p}, -\sqrt{p}\}\,.$$

Hence we obtain

$$P(S/\mathbb{F}_p; t) = (1 - pt^2)^2\,.$$

On the other hand, if $\chi(a) \neq 1$, we have

$$\begin{aligned}\{\alpha_1^2, \alpha_2^2, \alpha_3^2, \alpha_4^2\} &= \{-\omega J(\tilde{\chi}, \eta), -\omega^2 J(\tilde{\chi}^2, \eta), -\omega J(\tilde{\chi}, \eta^3), -\omega^2 J(\tilde{\chi}^2, \eta^3)\} \\ &= \{\omega p, \omega^2 p, \omega p, \omega^2 p\}\,,\end{aligned}$$

and therefore

$$\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} = \{\omega\sqrt{p}, -\omega\sqrt{p}, \omega^2\sqrt{p}, -\omega^2\sqrt{p}\}\,.$$

Hence we obtain

$$P(S/\mathbb{F}_p; t) = 1 + pt^2 + p^2 t^4\,.$$

3.5. Proof of (4). We have a prime decompostion $(p) = \mathfrak{q}\mathfrak{q}'$ in $\mathbb{Q}(\sqrt{3})$ ($\mathfrak{q} \neq \mathfrak{q}'$) since $p \equiv 11 \mod 12$. Moreover the prime ideals $\mathfrak{q}$ and $\mathfrak{q}'$ inert in the extension $\mathbb{Q}(e^{\frac{\pi i}{6}})/\mathbb{Q}(\sqrt{3})$, and we have a prime factorization $(p) = \mathfrak{q}\mathfrak{q}'$ in $\mathbb{Q}(e^{\frac{\pi i}{6}})$. Let χ and η denote the multiplicative character of $\mathbb{F}_{p^2}$ defined by $\alpha \mapsto \left(\frac{\alpha}{\mathfrak{q}}\right)_3$ and $\alpha \mapsto \left(\frac{\alpha}{\mathfrak{q}}\right)_4$, respectively.

By the definition, the Jacobi sum $J(\chi, \eta)$ is an integer in $\mathbb{Q}(e^{\frac{\pi i}{6}})$. We obtain a congruence relation

$$J(\chi, \eta) \equiv 0 \mod \mathfrak{q}\,,$$

applying Lemma 1.4 to $K = \mathbb{Q}(e^{\frac{\pi i}{6}})$, $\mathfrak{p} = \mathfrak{q}$, $n = 12$, $i = 4$, $j = 3$.

Define now $\sigma \in \mathrm{Gal}(\mathbb{Q}(e^{\frac{\pi i}{6}})/\mathbb{Q})$ by $\sigma(e^{\frac{\pi i}{6}}) = e^{\frac{5\pi i}{6}}$. Then the subfield $\mathbb{Q}(\sqrt{-1})$ of $\mathbb{Q}(e^{\frac{\pi i}{6}})$ is invariant under the action by σ, and $\sigma(\mathfrak{q}) = \mathfrak{q}'$. It follows that

$$\left(\frac{\alpha}{\mathfrak{q}'}\right)_3 = \left(\frac{\alpha}{\mathfrak{q}}\right)_3^{-1},\ \left(\frac{\alpha}{\mathfrak{q}'}\right)_4 = \left(\frac{\alpha}{\mathfrak{q}}\right)_4$$

for any $\alpha \in \mathbb{Z}[\sqrt{-1}]$. Hence we obtain a congruence relation

$$J(\chi, \eta) \equiv 0 \mod \mathfrak{q}',$$

applying Lemma 1.4 to $K = \mathbb{Q}(e^{\frac{\pi i}{6}})$, $\mathfrak{p} = \mathfrak{q}'$, $n = 12$, $i = 8$, $j = 3$.

Combining the two congruence relations, we obtain

$$J(\chi, \eta) \equiv 0 \mod p.$$

Hence we can conclude that

$$J(\chi, \eta) \in \{\pm p, \pm ip, \pm\omega p, \pm\omega^2 p, \pm i\omega p, \pm i\omega^2 p\}$$

since $|J(\chi, \eta)| = p$.

By Corollary 2.5, we have

$$\operatorname{Tr} J(\chi, \eta) \equiv -4 \mod 12.$$

On the other hand, we have

$$\operatorname{Tr}(p) = 4p,\ \operatorname{Tr}(-p) = -4p,\ \operatorname{Tr}(ip) = \operatorname{Tr}(-ip) = 0,$$

$$\operatorname{Tr}(\omega p) = \operatorname{Tr}(\omega^2 p) = -p,\ \operatorname{Tr}(-\omega p) = \operatorname{Tr}(-\omega^2 p) = p,$$

$$\operatorname{Tr}(i\omega p) = \operatorname{Tr}(i\omega^2 p) = \operatorname{Tr}(-i\omega p) = \operatorname{Tr}(-i\omega^2 p) = 0,$$

and therefore,

$$\operatorname{Tr}(p) \equiv -4 \mod 12,\ \operatorname{Tr}(p) \equiv 4 \mod 12,$$

$$\operatorname{Tr}(\omega p) = \operatorname{Tr}(\omega^2 p) \equiv 2 \mod 12,\ \operatorname{Tr}(-\omega p) = \operatorname{Tr}(-\omega^2 p) \equiv -2 \mod 12$$

since $p \equiv 11 \mod 12$. These imply

$$J(\chi, \eta) = J(\chi^2, \eta) = J(\chi, \eta^3) = J(\chi^2, \eta^3) = p.$$

Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be as above. For any $a \in F_p$, we have $\eta(a) = 1$ and $\chi(a) = 1$ since $p + 1 \equiv 0 \mod 12$. Hence, we have

$$\begin{aligned}\{\alpha_1^2, \alpha_2^2, \alpha_3^2, \alpha_4^2\} &= \{-J(\chi, \eta), -J(\chi^2, \eta), -J(\chi, \eta^3), -J(\chi^2, \eta^3)\} \\ &= \{-p, -p, -p, -p\},\end{aligned}$$

and therefore

$$\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} = \{i\sqrt{p}, -i\sqrt{p}, i\sqrt{p}, -i\sqrt{p}\}.$$

Hence we obtain

$$P(S/\mathbb{F}_p; t) = (1 + pt^2)^2.$$

3.6. Proof of (2). First note that the prime ideals (ρ) and $(\bar{\rho})$ of $\mathbb{Q}(\sqrt{-1})$ inert in the extension $\mathbb{Q}(e^{\frac{\pi i}{6}})/\mathbb{Q}(\sqrt{-1})$, and we have a prime factorization $(p) = (\rho)(\bar{\rho})$ in $\mathbb{Q}(e^{\frac{\pi i}{6}})$. Let χ and η denote the multiplicative character of $\mathbb{F}_{p^2}$ defined by $\alpha \mapsto \left(\frac{\alpha}{\rho}\right)_3$ and $\alpha \mapsto \left(\frac{\alpha}{\rho}\right)_4$, repsectively.

By the definition, the Jacobi sum $J(\chi, \eta)$ is an integer in $\mathbb{Q}(e^{\frac{\pi i}{6}})$. We obtain a congruence relation

$$J(\chi, \eta) \equiv 0 \mod \rho\,,$$

applying Lemma 1.4 to $K = \mathbb{Q}(e^{\frac{\pi i}{6}})$ and $n = 12$, $i = 4$, $j = 3$.

In the next paragraph we shall show

$$(\#) \qquad J(\chi, \eta) \equiv 0 \mod \rho^2\,.$$

Admitting (#), we verify the assertion. We can conclude that

$$J(\chi, \eta) \in \{\pm\rho^2, \pm i\rho^2, \pm\omega\rho^2, \pm\omega^2\rho^2, \pm i\omega\rho^2, \pm i\omega^2\rho^2\}$$

since $|J(\chi, \eta)| = |\rho^2| = p$.

By Corollary 2.5, we have

$$\mathrm{Tr}(J(\chi, \eta)) \equiv -4 \mod 12\,.$$

On the other hand, we have

$$\mathrm{Tr}(\rho^2) = 4(C^2 - D^2),\ \mathrm{Tr}(i\rho^2) = -8CD,\ \mathrm{Tr}(\omega^2\rho^2) = \mathrm{Tr}(\omega\rho^2) = -2(C^2 - D^2)\,,$$

$$\mathrm{Tr}(-\rho^2) = -4(C^2 - D^2),\ \mathrm{Tr}(-i\rho^2) = 8CD,\ \mathrm{Tr}(-\omega^2\rho^2) = \mathrm{Tr}(-\omega\rho^2) = 2(C^2 - D^2)\,,$$

$$\mathrm{Tr}(i\omega^2\rho^2) = \mathrm{Tr}(i\omega\rho^2) = 4CD,\ \mathrm{Tr}(-i\omega^2\rho^2) = \mathrm{Tr}(-i\omega\rho^2) = -4CD\,.$$

Then we obtain

$$\mathrm{Tr}(\rho^2) \equiv 0 \mod 12,\ \mathrm{Tr}(i\rho^2) \equiv 4 \mod 12,\ \mathrm{Tr}(\omega^2\rho^2) = \mathrm{Tr}(\omega\rho^2) \equiv 6 \mod 12\,,$$

$$\mathrm{Tr}(-\rho^2) \equiv 0 \mod 12,\ \mathrm{Tr}(-i\rho^2) \equiv -4 \mod 12,\ \mathrm{Tr}(-\omega^2\rho^2) = \mathrm{Tr}(-\omega\rho^2) \equiv 6 \mod 6\,,$$

$$\mathrm{Tr}(i\omega^2\rho^2) = \mathrm{Tr}(i\omega\rho^2) \equiv 4 \mod 12,\ \mathrm{Tr}(-i\omega^2\rho^2) = \mathrm{Tr}(-i\omega\rho^2) \equiv -4 \mod 12$$

since $C \equiv 1 \mod 6$ and $D \equiv 4 \mod 6$.

Now let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ as be avobe. Then we have

$$\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$$

since $\#X(\mathbb{F}_p) = \#E(\mathbb{F}_p) = p + 1$ as is shown in Example 1.6 and 2.2. Hence we have

$$\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} = \{\alpha = \alpha_1, \bar{\alpha}, -\alpha, -\bar{\alpha}\}\,,$$

and therefore,

$$\{\alpha_1^2, \alpha_2^2, \alpha_3^2, \alpha_4^2\} = \{\alpha^2, \bar{\alpha}^2, \alpha^2, \bar{\alpha}^2\}\,.$$

Hence we can exclude the possibility $J(\chi, \eta) \in \{-i\omega^2\rho^2, -i\omega\rho^2\}$. Then we have gotten

$$J(\chi, \eta) = J(\chi^2, \eta) = -i\rho^2,\ J(\chi, \eta^3) = J(\chi^2, \eta^3) = i\bar{\rho}^2\,.$$

For any $a \in \mathbb{F}_p$, we have $\eta(a) = \left(\frac{a}{p}\right)$ and $\chi(a) = 1$ since $p + 1 \equiv 6 \mod 12$. Hence, if $\left(\frac{a}{p}\right) = 1$, we have

$$\begin{aligned}\{\alpha_1^2, \alpha_2^2, \alpha_3^2, \alpha_4^2\} &= \{-J(\chi, \eta), -J(\chi^2, \eta), -J(\chi, \eta^3), -J(\chi^2, \eta^3)\} \\ &= \{i\rho^2, i\rho^2, -i\bar{\rho}^2, -i\bar{\rho}^2\},\end{aligned}$$

and therefore

$$\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} = \{e^{\frac{\pi i}{4}}(C + Di), -e^{\frac{\pi i}{4}}(C + Di), e^{-\frac{\pi i}{4}}(C - Di), -e^{-\frac{\pi i}{4}}(C - Di)\}.$$

Hence we obtain

$$P(S/\mathbb{F}_p; t) = 1 + 4CDt^2 + p^2t^4.$$

On the other hand, if $\left(\frac{a}{p}\right) = -1$, we have

$$\{\alpha_1^2, \alpha_2^2, \alpha_3^2, \alpha_4^2\} = \{J(\chi, \eta), J(\chi^2, \eta), J(\chi, \eta^3), J(\chi^2, \eta^3)\} = \{-i\rho^2, -i\rho^2, i\bar{\rho}^2, i\bar{\rho}^2\},$$

and therefore

$$\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} = \{e^{-\frac{\pi i}{4}}(C + Di), -e^{-\frac{\pi i}{4}}(C + Di), e^{\frac{\pi i}{4}}(C - Di), -e^{\frac{\pi i}{4}}(C - Di)\}.$$

Hence we obtain

$$P(S/\mathbb{F}_p; t) = 1 - 4CDt^2 + p^2t^4.$$

3.7. Proof of (#). We have $J(\chi, \eta) \equiv 0 \mod \rho^2$ or $J(\chi, \eta) \equiv 0 \mod p$ since $J(\chi, \eta)J(\chi^2, \eta^3) = p^2$ and $J(\chi, \eta) \equiv 0 \mod \rho$.

Assume that we have $J(\chi, \eta) \equiv 0 \mod p$. Then we have

$$J(\chi, \eta) = J(\chi^2, \eta) = J(\chi, \eta^3) = J(\chi^2, \eta^3) = p,$$

repeating the argument in 3.5. Take $a \in \mathbb{F}_{p^2}$ so that $\chi(a) = \omega$ and $\eta(a) = 1$. Then we have

$$(*) \qquad \mathrm{Tr}(\omega J(\chi, \eta)) = \mathrm{Tr}(\omega p) = -2p \equiv 2 \mod 12.$$

Put now

$$R = \left\{(\alpha, \beta) \in \mathbb{F}_{p^2}^2 \,;\ \beta^2 = \alpha^3 + a,\ \left(\frac{\beta}{\rho}\right)_2 = 1\right\},$$

$$S = \left\{(\alpha, \beta) \in \mathbb{F}_{p^2}^2 \,;\ \beta^2 = \alpha^3 + a,\ \left(\frac{\beta}{\rho}\right)_2 = -1\right\},$$

$$T = \left\{(\alpha, \beta) \in \mathbb{F}_{p^2}^2 \,;\ \beta^2 = \alpha^3 + a,\ \left(\frac{\beta}{\rho}\right)_2 = 0\right\}$$

and

$$r = \#R,\ s = \#S,\ t = \#T.$$

Then we obtain

$$\sum_{\substack{(\alpha,\beta)\in\mathbb{F}_{p^2}^2 \\ \beta^2=\alpha^3+a}} \left(\frac{a}{\rho}\right)_2 = r - s = 2r + t - \#E(\mathbb{F}_{p^2}) + 1\,.$$

as in the proof of Lemma 2.4.

Note now there exists $c \in \mathbb{F}_{p^2}$ such that $c^4 = a$ since $\eta(a) = 1$. Then we have a partition

$$R = \left\{(\alpha,\beta) \in (\mathbb{F}_{p^2}^{\times})^2\ ;\ \beta^2 = \alpha^3 + a,\ \left(\frac{\beta}{\rho}\right)_2 = 1\right\} \cup \{(0, \pm c^2)\}\,,$$

and therefore, we have $r \equiv 2 \mod 6$ since the group $\boldsymbol{\mu}_3 \times \boldsymbol{\mu}_2$ acts faithfully on $R - \{(0, \pm c^2)\}$ by $(\zeta,\theta)(\alpha,\beta) = (\zeta\alpha, \theta\beta)$. We have also $t = 0$ since $\chi(a) \neq 1$.

Moreover we have $\#E(\mathbb{F}_{p^2}) = p^2 + 1 + \omega p + \omega^2 p = p^2 - p + 1 \equiv -3 \mod 12$. Summing up, we obtain

$$\sum_{\substack{(\alpha,\beta)\in\mathbb{F}_{p^2}^2 \\ \beta^2=\alpha^3+a}} \left(\frac{a}{\rho}\right)_2 = 2r + t - \#E(\mathbb{F}_p) + 1 \equiv 8 \mod 12\,.$$

This contradicts to $(*)$ since

$$\sum_{\substack{(\alpha,\beta)\in\mathbb{F}_{p^2}^2 \\ \beta^2=\alpha^3+a}} \left(\frac{a}{\rho}\right)_2 = \mathrm{Tr}(\omega J(\chi,\eta))\,.$$

REMARK 3.8. Let p a prime number ≥ 5. Let X denote the non-singular complete curve defined by $y^4 = x^3 + 1$ over $\mathbb{F}_p$, and E the elliptic curve defined by $y^2 = x^3 + 1$ over $\mathbb{F}_p$. Put $S = \mathrm{Coker}[E \to J(X)]$.

If $p \equiv 1 \mod 12$, then S is isogenous to the self-product of an ordinary elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-1})$ over $\mathbb{F}_p$.

If $p \equiv 5 \mod 12$, then S is isogenous to the self-product of an ordinary elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-1})$ over $\mathbb{F}_{p^2}$. However S is simple over $\mathbb{F}_p$.

If $p \equiv 7 \mod 12$, then S is isogenous to the self-product of a supersingular elliptic curve over $\mathbb{F}_{p^2}$. However S is simple over $\mathbb{F}_p$.

If $p \equiv 11 \mod 12$, then S is isogenous to the self-product of a supersingular elliptic curve over $\mathbb{F}_p$.

REMARK 3.9. We will get a clearer view from a ropeway, referring to Stickelberger's theorem and to results on the isogeny decomposition of the Jacobian variety of a Fermat curve ([1], [4]). However we have chosen a more elementary method in this article, climbing step by step.

References

[1] N. Aoki, *Simple factors of the Jacobian of a Fermat curve and the Picard number of a product of Fermat curves*, Amer. J. Math. 113 (1991), 779–833.

[2] B. C. Berndt, R. J. Evans and K. S. Williams, Gauss and Jacobi sums (1998), Wiley-Interscience Publication, New York.

[3] H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. 172 (1934), 151–182.

[4] C. G. Schmidt, Arithmetik Abelscher Varietäten mit komplexer Multiplikation, Lecture Notes in Math. 1082 (1984), Springer-Verlag, Berlin.

[5] J. H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Math. 106 (1985) , Springer-Verlag, Berlin.

Department of Mathematics,
Chuo University, 1–13–27 Kasuga,
Bunkyo-ku, Tokyo 112–8551, Japan
E-mail: ozaki@gug.math.chuo-u.ac.jp